Sources d'identité

Les sources d’identité sont des serveurs et des bases de données qui définissent les comptes utilisateur. Vous pouvez utiliser ces informations de diverses manières, par exemple pour fournir l’identité de l’utilisateur associée à une adresse IP ou authentifier des connexions VPN d’accès à distance ou l’accès à Firepower Device Manager.

Les rubriques suivantes expliquent comment définir les sources d'identité. Vous utiliserez ensuite ces objets lors de la configuration des services qui nécessitent une source d’identité.

À propos des sources d’identité

Les sources d’identité sont les serveurs et bases de données AAA qui définissent les comptes utilisateur pour les membres de votre organisation. Vous pouvez utiliser ces informations de diverses manières, par exemple en fournissant l’identité de l’utilisateur associée à une adresse IP, ou pour l’authentification des connexions VPN d’accès à distance ou de l’accès à Firepower Device Manager.

Utilisez la page **Objects (Objects)** > **Identity Sources (Sources d’identité)** pour créer et gérer vos sources. Vous utiliserez ensuite ces objets lors de la configuration des services qui nécessitent une source d’identité.

Voici les sources d’identité prises en charge et leurs utilisations :

Domaine d’identité Active Directory (AD)

Active Directory fournit des informations sur le compte d’utilisateur et l’authentification. Consultez Domaine d’identité Active Directory (AD), à la page 3.

Vous pouvez utiliser cette source aux fins suivantes :

- Le VPN d’accès à distance, comme source d’identité principale. Vous pouvez utiliser AD conjointement avec un serveur RADIUS.
- Politique d’identité, pour l’authentification active et comme source d’identité d’utilisateur utilisée avec l’authentification passive.

Séquence de domaine AD (Active Directory)

Une séquence de domaine AD est une liste ordonnée d'objets de domaine AD. Les séquences de domaine sont utiles si vous gérez plusieurs domaines AD dans votre réseau. Consultez Configuration d'une séquence de domaine AD, à la page 7.

Vous pouvez utiliser cette source aux fins suivantes :

- Identity policy (stratégie d'identité), en tant que source d'identité d'utilisateur utilisée avec l'authentification passive. L'ordre des domaines dans la séquence détermine la façon dont le système détermine l'identité de l'utilisateur dans les rares cas de conflit.

Cisco Identity Services Engine (ISE) ou Cisco Identity Services Engine Passive Identity Connector (ISE PIC)

Si vous utilisez ISE, vous pouvez intégrer le périphérique Cisco Firewall Threat Defense à votre déploiement ISE. Consultez Identity Services Engine (ISE), à la page 14.

Vous pouvez utiliser cette source aux fins suivantes :

- Identity policy (stratégie d'identité), en tant que source d'identité passive pour collecter l'identité de l'utilisateur auprès d'ISE.

Serveurs RADIUS, Groupes de serveurs RADIUS

Si vous utilisez des serveurs RADIUS, vous pouvez également les utiliser avec le Firepower Device Manager. Vous devez définir chaque serveur comme un objet distinct, puis les placer dans des groupes de serveurs (où les serveurs d'un groupe donné sont des copies les uns des autres). Vous affectez le groupe de serveurs à des fonctionnalités, vous n'affectez pas de serveurs individuels. Consultez Serveurs et groupes RADIUS, à la page 9.

Vous pouvez utiliser cette source aux fins suivantes :

- Le VPN d'accès à distance, en tant que source d'identité pour l'authentification, et pour l'autorisation et la comptabilité. Vous pouvez utiliser AD conjointement avec un serveur RADIUS.
- La politique d'identité, en tant que source d'identité passive pour collecter l'identité de l'utilisateur à partir des connexions VPN d'accès à distance.
- Authentification extérieure pour les utilisateurs Firepower Device Manager ou Cisco Firewall Threat Defense de gestion de l'interface de ligne de commande. Vous pouvez prendre en charge plusieurs utilisateurs de gestion avec différents niveaux d'autorisation. Ces utilisateurs peuvent se connecter au système à des fins de configuration et de surveillance des périphériques.

Serveur SAML

Security Assertion Markup Language 2.0 (SAML 2.0) est une norme ouverte pour l'échange de données d'authentification et d'autorisation entre les parties, en particulier un fournisseur d'identité (IdP) et un fournisseur de services (SP).

Vous pouvez utiliser cette source aux fins suivantes :

- VPN d'accès à distance, en tant que source d'authentification de connexion unique (SSO).

Source d'identité locale

Il s'agit de la base de données des utilisateurs locaux, qui comprend les utilisateurs que vous avez définis dans le Firepower Device Manager. Sélectionnez **Objects (Objets)** > **Users (Utilisateurs)** pour gérer les comptes d'utilisateurs dans cette base de données. Consultez Utilisateurs locaux, à la page 20.

Remarque La base de données de la source d'identité locale n'inclut pas les utilisateurs que vous configurez dans l'interface de ligne de commande pour l'accès à l'interface de ligne de commande (à l'aide de la commande **configure user add**). Les utilisateurs de l'interface de ligne de commande sont totalement distincts de ceux que vous créez dans le Firepower Device Manager.

Vous pouvez utiliser cette source aux fins suivantes :

- VPN d'accès à distance, comme source d'identité principale ou de secours.
- Politique d'identité, en tant que source d'identité passive pour collecter l'identité de l'utilisateur à partir des connexions VPN d'accès à distance.

Domaine d'identité Active Directory (AD)

Microsoft Active Directory (AD) définit les comptes utilisateur. Vous pouvez créer un domaine d'identité AD pour un domaine Active Directory. Les rubriques suivantes expliquent comment définir un domaine d'identité AD.

Serveurs d'annuaire pris en charge

Vous pouvez utiliser Microsoft Active Directory (AD) sur Windows Server 2012, 2016 et 2019.

Tenez compte des éléments suivants concernant la configuration de votre serveur :

- Si vous souhaitez effectuer un contrôle utilisateur sur des groupes d'utilisateurs ou sur les utilisateurs de groupes, vous devez configurer les groupes d'utilisateurs sur le serveur d'annuaire. Le système ne peut pas effectuer le contrôle des groupes d'utilisateurs si le serveur organise les utilisateurs selon une hiérarchie d'objets de base.
- Le serveur d'annuaire doit utiliser les noms de champ répertoriés dans le tableau suivant pour que le système puisse récupérer les métadonnées utilisateur des serveurs pour ce champ :

Métadonnées	Champ Active Directory
Nom d'utilisateur LDAP	samaccountname
prénom	givenname
nom	sn
adresse courriel	mail userprincipalname (si courriel n'a aucune valeur)
department	department distinguishedname (si le service n'a aucune valeur)
numéro de téléphone	telephonenumber

Limites relatives au nombre d'utilisateurs

Firepower Device Manager peut télécharger des informations sur un maximum de 50,000 utilisateurs à partir du serveur d'annuaire.

Si votre serveur d'annuaire comprend plus de 50 000 comptes utilisateur, vous ne verrez pas tous les noms possibles lors de la sélection des utilisateurs dans une règle d'accès ou lors de l'affichage des informations de tableau de bord basé sur l'utilisateur. Vous pouvez écrire des règles uniquement sur les noms qui ont été téléchargés.

La limite s'applique également aux noms associés aux groupes. Si un groupe compte plus de 50 000 membres, seuls les noms des 50 000 téléchargés peuvent être associés à l'appartenance au groupe.

Détermination du DN de base du répertoire

Lorsque vous configurez les propriétés d'annuaire, vous devez préciser le nom distinctif (DN) commun de base pour les utilisateurs et les groupes. La base est définie dans votre serveur d'annuaire et diffère d'un réseau à l'autre. Vous devez entrer les bases avec exactitude pour que les politiques d'identité fonctionnent. Si la base est incorrecte, le système ne peut pas déterminer les noms d'utilisateur ou de groupe, de sorte que les politiques basées sur l'identité seront inutilisables.

Astuces Pour obtenir les bonnes bases, consultez l'administrateur responsable des serveurs d'annuaire.

Pour le répertoire actif (Active Directory), vous pouvez déterminer les bases exactes en vous connectant au serveur Active Directory en tant qu'administrateur de domaine et en utilisant la commande **dsquery** à l'invite de commande pour déterminer les bases. Voici la marche à suivre :

Point de départ de la recherche selon l'utilisateur

Entrez la commande **dsquery user** avec un nom d'utilisateur connu (partiel ou complet) pour déterminer le nom distinctif de base. Par exemple, la commande suivante utilise le nom partiel « John* » pour obtenir des informations pour tous les utilisateurs commençant par « John ».

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

Le DN de base serait « DC=csc-lab,DC=example,DC=com ».

Point de départ de la recherche selon le groupe

Entrez la commande **dsquery group** avec un nom de groupe connu pour déterminer le nom distinctif de base. Par exemple, la commande suivante utilise le nom de groupe « Employees » pour obtenir le nom distinctif :

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

Le DN de base du groupe serait « DC=csc-lab,DC=example,DC=com ».

Vous pouvez également utiliser le programme ADSI Edit pour parcourir la structure Active Directory (**Start (démarrer)** > **Run (exécuter)** > **adsiedit.msc**). Dans ADSI Edit, cliquez avec le bouton droit de la souris sur

n'importe quel objet, comme une unité organisationnelle, un groupe ou un utilisateur, puis choisissez **Properties** (propriétés) pour afficher le nom distinctif. Vous pouvez ensuite copier la chaîne de valeurs DC comme base.

Pour vérifier que vous avez établi la bonne base :

1. Sous les propriétés du répertoire, cliquez sur le bouton Test Connection (tester la connexion) pour vérifier la connectivité. Réglez les problèmes (le cas échéant) et enregistrez les propriétés du répertoire.
2. Validez les modifications apportées à l'appareil.
3. Créez une règle d'accès, sélectionnez l'onglet **Users** (utilisateurs) et essayez d'ajouter des noms d'utilisateur et de groupe connus à partir du répertoire. Vous devriez voir des suggestions automatiques lorsque vous tapez des entrées pour les utilisateurs et les groupes dans le domaine qui contient le répertoire. Si les suggestions apparaissent dans une liste déroulante, le système a pu interroger le répertoire avec succès. Si vous ne voyez aucune suggestion et que vous êtes certain que la chaîne que vous avez saisie doit apparaître dans un nom d'utilisateur ou de groupe, vous devez corriger le point de départ de la recherche en conséquence.

Configuration des domaines d'identité AD

Un domaine d'identité est un serveur de répertoire ainsi que d'autres attributs requis pour fournir des services d'authentification. Le serveur de répertoire contient des renseignements sur les utilisateurs et les groupes d'utilisateurs qui sont autorisés à accéder à votre réseau.

Pour Active Directory, un domaine équivaut à un domaine Active Directory. Créez des domaines distincts pour chaque domaine AD que vous devez prendre en charge.

Les domaines d'identité sont utilisés dans les politiques suivantes :

- Identité : le domaine d'identité fournit des informations sur l'identité de l'utilisateur et l'appartenance au groupe, que vous pouvez ensuite utiliser dans les règles de contrôle d'accès. Le système télécharge chaque jour les informations mises à jour sur tous les utilisateurs et groupes pendant la dernière heure du jour (UTC). Le serveur de répertoire doit être accessible à partir de l'interface de gestion.
- VPN d'accès à distance : le domaine d'identité fournit des services d'authentification, qui déterminent si une connexion est autorisée. Le serveur de répertoire doit être accessible à partir de l'interface externe du VPN d'accès à distance.
- Contrôle d'accès, déchiffrement SSL : vous pouvez sélectionner le domaine d'identité dans les critères utilisateur pour appliquer la règle à tous les utilisateurs du domaine.

Collaborez avec votre administrateur de répertoire pour obtenir les valeurs requises pour configurer les propriétés du serveur de répertoire.

Remarque Si le serveur de répertoire ne se trouve pas sur un réseau associé ou n'est pas disponible via la route par défaut, créez une route statique pour le serveur. Sélectionnez **Device (Périphérique)** > **Routing (Routage)** > **View Configuration (Afficher la configuration)** pour créer des routes statiques.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de domaine d'identité lorsque vous modifiez une propriété de domaine, en cliquant sur le lien **Create New Identity Realm** (Créer un nouveau domaine d'identité) affiché dans la liste d'objets.

Avant de commencer

Vérifiez que les paramètres d'horloge sont uniformes pour les serveurs d'annuaire, le périphérique Firewall Threat Defense et les clients. Un décalage temporel entre ces périphériques peut empêcher l'authentification de l'utilisateur réussie. « cohérence » signifie que vous pouvez utiliser différents fuseaux horaires, mais que l'heure doit être la même pour ces fuseaux horaires; par exemple, 10 h HNP = 13 h HNE.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez (Domaine d'identité)**Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un domaine AD, cliquez sur **+** > **AD**.
- Pour modifier un domaine, cliquez sur l'icône de modification ( ) du domaine.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés de base du domaine.

- **Name** (nom) : Nom du domaine de répertoire.
- **Type** : Type de serveur d'annuaire. Active Directory est le seul type pris en charge et vous ne pouvez pas modifier ce champ.
- **Directory Username** (nom d'utilisateur), **Directory Password** (mot de passe d'annuaire) : nom d'utilisateur et mot de passe uniques pour un utilisateur disposant des droits appropriés sur les informations utilisateur que vous souhaitez récupérer. Pour Active Directory, l'utilisateur n'a pas besoin d'avoir des privilèges élevés. Vous pouvez préciser n'importe quel utilisateur dans le domaine. Le nom d'utilisateur doit être complet; par exemple, Administrateur@exemple.com (pas simplement Administrateur).

  Remarque
  Le système génère ldap-login-dn et ldap-login-password à partir de ces informations. Par exemple, Administrateur@exemple.com se traduit par cn=administrator,cn=users,dc=example,dc=com. Notez que cn=users fait toujours partie de cette traduction; vous devez donc configurer l'utilisateur que vous précisez ici sous le nom usuel du dossier « users ».

- **Base DN** (base DN) : L'arborescence pour faire des recherches ou requêtes d'informations sur les utilisateurs et les groupes, c'est-à-dire le parent commun des utilisateurs et des groupes. Par exemple, cn=users,dc=example,dc=com. Pour en savoir plus sur la recherche du DN de base, consultez Détermination du DN de base du répertoire, à la page 4.
- **AD Primary Domain** (domaine principal AD) : le nom de domaine complet d'Active Directory que le périphérique doit joindre.' Par exemple, exemple.com.

Étape 4 Configurez les propriétés du serveur d'annuaire.

- **Hostname/IP Address** (nom d'hôte/adresse IP) : le nom d'hôte ou l'adresse IP du serveur d'annuaire. Si vous utilisez une connexion chiffrée avec le serveur, vous devez saisir le nom de domaine complet, et non l'adresse IP.

- **Port** : le numéro de port utilisé pour les communications avec le serveur. La valeur par défaut est 389. Utilisez le port 636 si vous sélectionnez LDAPS comme méthode de chiffrement.
- **Encryption** (chiffrement) : Pour utiliser une connexion chiffrée pour le téléchargement des informations sur les utilisateurs et les groupes, sélectionnez la méthode souhaitée, **STARTTLS** ou **LDAPS**. La valeur par défaut est **None** (aucun), ce qui signifie que les informations relatives aux utilisateurs et aux groupes sont téléchargées en texte en clair.
  - **STARTTLS** négocie la méthode de chiffrement et utilise la méthode la plus efficace prise en charge par le serveur d'annuaire. Utilisez le port 389. Cette option n'est pas prise en charge si vous utilisez le domaine pour le VPN d'accès à distance.
  - **LDAPS** nécessite LDAP sur SSL. Utilisez le port 636.
- **Trusted CA Certificate** (certificat CA de confiance) : Si vous sélectionnez une méthode de chiffrement, téléchargez un certificat d'autorité de certification (CA) pour activer une connexion de confiance entre le système et le serveur d'annuaire. Si vous utilisez un certificat pour vous authentifier, le nom du serveur dans le certificat doit correspondre au nom d'hôte ou à l'adresse IP du serveur. Par exemple, si vous utilisez 10.10.10.250 comme adresse IP mais ad.exemple.com dans le certificat, la connexion échouera.

Étape 5 S'il y a plusieurs serveurs pour le domaine, cliquez sur **Add Another Configuration** (Ajouter une autre configuration) et saisissez les propriétés de chaque serveur supplémentaire.

Vous pouvez ajouter jusqu'à 10 serveurs AD au domaine. Ces serveurs doivent être des doublons les uns des autres et prendre en charge le même domaine AD.

Vous pouvez réduire et développer chaque entrée de serveur pour votre commodité. Les sections sont étiquetées avec le nom d'hôte ou l'adresse IP et le port.

Étape 6 Cliquez sur le bouton **Test** (Tester) pour vérifier que le système peut communiquer avec le serveur.

Le système utilise des processus et des interfaces distincts pour accéder au serveur. Vous pourriez donc obtenir des erreurs indiquant que la connexion fonctionne pour un type d'utilisation mais pas pour un autre, par exemple, disponibles pour les politiques d'identité mais pas pour le VPN d'accès à distance. Si le serveur n'est pas accessible, vérifiez que vous avez la bonne adresse IP et le bon nom d'hôte, que le serveur DNS dispose d'une entrée pour le nom d'hôte, etc. Vous devrez peut-être configurer une route statique pour le serveur. Pour en savoir plus, consultez Résolution de problèmes liés aux connexions du serveur de répertoire, à la page 8.

Étape 7 Cliquez sur **OK**.

Configuration d'une séquence de domaine AD

Vous pouvez utiliser une séquence de domaine AD dans une règle d'identité passive afin que le système tente de faire correspondre les utilisateurs de plusieurs serveurs AD. Dans une séquence de domaine AD, vous configurez une liste ordonnée de domaines AD où chaque serveur AD gère un domaine différent, par exemple engineering.example.com et marketing.example.com.

Les séquences de domaine sont utiles uniquement si vous prenez en charge plusieurs domaines AD, et les utilisateurs de différents domaines peuvent envoyer le trafic par l'intermédiaire du périphérique Firewall Threat Defense. Les domaines sont utilisés pour trouver l'identité d'une session utilisateur authentifiée passivement. L'ordre des domaines est utilisé pour résoudre les conflits d'identité, dans les rares cas où un conflit pourrait survenir.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer une séquence de domaine AD, cliquez sur **+** > **AD Realm Sequence (+ Séquence de domaine AD)**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés de séquence de domaine :

- **Name** (Nom) : le nom de l'objet.
- **Description** : ajoutez une description facultative.
- **AD Realms** (Domaines AD) : cliquez sur le signe **+** pour ajouter des objets de domaine AD à la séquence. Après avoir ajouté les domaines, cliquez sur et faites glisser et déposez les domaines dans la séquence ordonnée souhaitée.

Étape 4 Cliquez sur **OK**.

Vous pouvez maintenant sélectionner la séquence de domaine AD dans une règle d'identité passive.

Résolution de problèmes liés aux connexions du serveur de répertoire

Le système utilise différents processus pour communiquer avec votre serveur de répertoire en fonction de la fonctionnalité. Ainsi, une connexion pour les politiques d'identité peut fonctionner, alors qu'une connexion pour le VPN d'accès à distance peut échouer.

Ces processus utilisent différentes interfaces pour communiquer avec le serveur de répertoire. Vous devez assurer la connectivité à partir de ces interfaces.

- Interface de gestion, pour : les politiques d'identité.
- Interface de données, pour : le VPN d'accès à distance (interface externe).

Lorsque vous configurez le domaine d'identité, utilisez le bouton **Test** pour vérifier que la connexion peut fonctionner. Les messages de défaillance doivent indiquer la fonctionnalité qui présente des problèmes de connexion. Voici les problèmes généraux que vous pourriez rencontrer, selon les attributs d'authentification et la configuration du routage et de l'interface.

Problèmes d'authentification des utilisateurs de répertoire.

Si le problème est que le système n'a pas pu se connecter au serveur de répertoire en raison du nom d'utilisateur ou du mot de passe, assurez-vous que le nom et le mot de passe sont corrects et valides sur le serveur de répertoire. Pour Active Directory, l'utilisateur n'a pas besoin d'avoir des privilèges élevés. Vous pouvez préciser n'importe quel utilisateur dans le domaine. Le nom d'utilisateur doit être complet; par exemple, Administrateur@exemple.com (pas simplement Administrateur).

Le système génère également ldap-login-dn et ldap-login-password à partir des informations de nom d'utilisateur et de mot de passe. Par exemple, Administrateur@exemple.com se traduit par cn=administrator,cn=users,dc=example,dc=com. Notez que cn=users fait toujours partie de cette traduction; vous devez donc configurer l'utilisateur que vous précisez ici sous le nom usuel du dossier « users ».

Le serveur de répertoire est accessible par l'intermédiaire d'une interface de données.

Si le serveur de répertoire se trouve sur un réseau directement connecté à une interface de données (comme une interface GigabitEthernet) ou routable à partir d'un réseau directement connecté, vous devez vous assurer qu'une route existe entre l'interface de gestion virtuelle et le serveur de répertoire.

- L'utilisation de **data-interfaces** comme passerelle de gestion devrait permettre au routage de s'effectuer correctement.
- Si vous avez une passerelle explicite sur l'interface de gestion, ce routeur doit disposer d'une route vers le serveur de répertoire.
- Vous n'avez pas besoin de configurer une adresse IP sur l'interface de **diagnostic**, qui est l'interface physique utilisée par l'interface de gestion virtuelle. Toutefois, si vous configurez une adresse, ne configurez pas également une route statique (comme une route par défaut) qui redirigerait le trafic destiné au serveur de répertoire vers l'interface de diagnostic.
- S'il y a un routeur entre le réseau directement connecté et le réseau qui héberge le serveur de répertoire, configurez une route statique pour le serveur de répertoire dans (**Device (Périphérique)** > **Routing (Routage)**).
- Vérifiez que l'interface de données dispose de l'adresse IP et du masque de sous-réseau appropriés.

Le serveur de répertoire est accessible par l'intermédiaire de l'interface physique de gestion.

Si le serveur de répertoire se trouve sur le réseau directement connecté à l'interface physique de gestion (comme Management0/0) ou routable à partir de ce réseau, vous devez effectuer les opérations suivantes :

- Configurez une adresse IPv4 pour l'interface de gestion (dont le nom logique est **diagnostic**) dans **Device (Périphérique)** > **Interfaces**. L'adresse IP doit se trouver sur le même sous-réseau que l'adresse de gestion virtuelle (**Device (Périphérique)** > **System Settings (Paramètres du système)** > **Management Interface (Interface de gestion)**).
- S'il y a un routeur entre le serveur de répertoire et l'interface de gestion, configurez une route pour le serveur de répertoire dans **Device (Périphérique)** > **Routing (Routage)** pour l'interface **diagnostic**.
- Vérifiez que les interfaces de diagnostic et de gestion possèdent l'adresse IP et le masque de sous-réseau appropriés.

Le serveur de répertoire se trouve sur un réseau externe.

Si le serveur de répertoire se trouve sur un réseau situé de l'autre côté de l'interface externe (liaison ascendante), vous devrez peut-être configurer une connexion VPN de site à site. Pour la procédure détaillée, consultez Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance.

Serveurs et groupes RADIUS

Vous pouvez utiliser les serveurs RADIUS pour authentifier et autoriser les connexions VPN d'accès à distance, ainsi que le Firepower Device Manager et les utilisateurs d'administration de l'interface de ligne de commande

Cisco Firewall Threat Defense. Par exemple, si vous utilisez également Moteur de services de vérification des identités de Cisco (ISE) et son serveur RADIUS, vous pouvez utiliser ce serveur avec la fonction Firepower Device Manager.

Lorsque vous configurez une fonctionnalité pour utiliser des serveurs RADIUS, vous sélectionnez un groupe RADIUS plutôt que des serveurs individuels. Un groupe RADIUS est un ensemble de serveurs RADIUS qui sont des copies les uns des autres. Si un groupe a plusieurs serveurs, ils forment une chaîne de serveurs de sauvegarde pour assurer la redondance au cas où un serveur deviendrait indisponible. Mais même si vous n'avez qu'un seul serveur, vous devez créer un groupe comptant un seul membre pour configurer la prise en charge de RADIUS pour une fonctionnalité.

Les rubriques suivantes expliquent comment configurer des serveurs et des groupes RADIUS, afin qu'ils puissent être utilisés dans les fonctionnalités prises en charge.

Configurer les serveurs RADIUS

Les serveurs RADIUS fournissent des services AAA (authentification, autorisation et comptabilité). Si vous utilisez des serveurs RADIUS pour authentifier et autoriser les utilisateurs, vous pouvez utiliser ces serveurs avec le Firepower Device Manager.

Après avoir créé des objets pour chacun de vos serveurs RADIUS, créez des groupes de serveurs RADIUS pour contenir chaque groupe de serveurs en double.

Avant de commencer

Si vous souhaitez configurer une liste de contrôle d'accès de redirection pour le VPN d'accès à distance, vous devez utiliser la console d'interface en ligne de commande Smart (Smart CLI) pour créer la liste de contrôle d'accès étendue avant de créer ou de modifier l'objet serveur. Vous ne pouvez pas créer la liste de contrôle d'accès lors de la modification de l'objet.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur **+** > **RADIUS Server** (Serveur RADIUS).
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Name** (Nom) : le nom de l'objet. Il n'est pas nécessaire que cela corresponde à quoi que ce soit configuré sur le serveur.
- **Nom ou adresse IP du serveur** : nom d'hôte complet (FQDN) ou adresse IP du serveur. Par exemple, radius.example.com ou 10.100.10.10.
- **Authentication Port** (Port d'authentification) : le port sur lequel l'authentification et l'autorisation RADIUS sont effectuées. Par défaut, c'est 1812 .

- **Timeout** : la durée, de 1 à 300 secondes, pendant laquelle le système attend une réponse du serveur avant d'envoyer la demande au serveur suivant. La valeur par défaut est de 10 secondes. Si vous utilisez ce serveur comme source d'authentification secondaire pour le VPN d'accès à distance, par exemple, pour demander un jeton d'authentification, augmentez ce délai d'authentification à 60 secondes au moins. Cela donne le temps à l'utilisateur d'obtenir et de saisir le jeton.
- **Server Secret Key** (Clé secrète du serveur) : (Facultatif.) le code secret partagé qui est utilisé pour chiffrer les données entre le dispositif Cisco Firewall Threat Defenseet le serveur RADIUS. La clé est une chaîne de caractères alphanumériques sensible à la casse et composé de jusqu'à 64 caractères, espaces exclus. La clé doit commencer par un caractère alphanumérique ou un trait de soulignement et peut contenir les caractères spéciaux : $ - _ . + @. Cette chaîne de caractères doit correspondre à la clé configurée sur le serveur RADIUS. Si vous ne configurez pas de clé secrète, la connexion ne sera pas chiffrée.

Étape 4 (Facultatif) Si vous utilisez le serveur pour la configuration Change of Authorization du VPN d'accès à distance, vous pouvez cliquer sur le lien **RA VPN Only** (VPN d'accès à distance uniquement) et configurer les options suivantes.

- **ACL de redirection** : sélectionnez la liste de contrôle d'accès étendue à utiliser pour la liste de contrôle d'accès de redirection du VPN d'accès à distance. Créez ces listes de contrôle d'accès au moyen de l'objet Smart CLI **Extended Access List** (liste d'accès étendue Smart CLI) dans la page **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** > **Smart CLI** > **Objects (Objets)**.

  L'objectif de la liste de contrôle d'accès de redirection est d'envoyer le trafic initial à Cisco Identity Services Engine (ISE) afin qu'ISE puisse évaluer la posture du client. La liste de contrôle d'accès doit envoyer le trafic HTTPS à ISE, mais pas le trafic déjà destiné à ISE ou le trafic dirigé vers un serveur DNS pour la résolution de nom. Pour obtenir un exemple, consultez Configurer Change of Authorization (modification d'autorisation) sur le périphérique Firewall Threat Defense.
- **Interface utilisée pour la connexion au serveur RADIUS** : quelle interface utiliser lors de la communication avec le serveur. Si vous sélectionnez **Résoudre par recherche de route**, le système utilise toujours la table de routage pour déterminer l'interface à utiliser. Si vous sélectionnez **Sélectionner manuellement l'interface**, le système utilisera toujours l'interface que vous sélectionnez.

  Si vous configurez la modification d'autorisation, vous devez sélectionner une interface spécifique pour que le système puisse activer correctement l'écouteur CoA sur celle-ci.

  Si le serveur se trouve sur le même réseau que l'adresse de gestion, ce qui signifie que vous sélectionnerez l'interface de diagnostic, vous devez également configurer une adresse IP sur l'interface de diagnostic. Il n'est pas suffisant d'avoir une adresse IP de gestion. Accédez à **Device (Périphérique)** > **Interfaces**, et configurez une adresse IP sur l'interface de diagnostic qui se trouve sur le même sous-réseau que l'adresse IP de gestion.

  Si vous utilisez également ce serveur pour l'accès administratif Firepower Device Manager, cette interface est ignorée. Les tentatives d'accès administratif sont toujours authentifiées au moyen de l'adresse IP de gestion.

Étape 5 (Facultatif, lors de la modification de l'objet uniquement.) Cliquez sur **Test** pour vérifier si le système peut se connecter au serveur.

Vous êtes alors invité(e) à saisir un nom d'utilisateur et un mot de passe. Le test vérifie si le serveur peut être contacté et, si oui, que le nom d'utilisateur peut être authentifié.

Étape 6 Cliquez sur **OK**.

Configurer les groupes de serveurs RADIUS

Un groupe de serveurs RADIUS contient un ou plusieurs objets serveur RADIUS. Les serveurs d'un groupe doivent être des copies les uns des autres. Ces serveurs forment une chaîne de serveurs de sauvegarde, de sorte que si le premier serveur n'est pas disponible, le système peut essayer le serveur suivant dans la liste.

Lorsque vous configurez la prise en charge de RADIUS dans une fonctionnalité, vous devez sélectionner un groupe de serveurs. Ainsi, même si vous n'avez qu'un seul serveur RADIUS, vous devez créer un groupe de serveurs pour le contenir.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur **+** > **RADIUS Server Group** (Groupe de serveurs RADIUS).
- Pour modifier un objet, cliquez sur l'icône de modification () de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille () de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Name** (Nom) : le nom de l'objet. Cela ne doit pas correspondre à ce qui est configuré sur les serveurs.
- **Dead Time** (Temps mort) : les serveurs défaillants ne sont réactivés que lorsque tous les serveurs sont tombés en panne. Le temps mort est le temps d'attente, de 0 à 1440 minutes, après l'échec du dernier serveur avant la réactivation de tous les serveurs. Le temps mort s'applique uniquement si vous configurez le secours pour la base de données locale; l'authentification est tentée localement jusqu'à l'expiration du temps mort. La valeur par défaut est 10 minutes.
- **Maximum Failed Attempts** (Nombre maximal de tentatives échouées) : le nombre de transactions AAA échouées (c'est-à-dire de demandes ne recevant pas de réponse) envoyées à un serveur RADIUS du groupe avant d'essayer le serveur suivant. Vous pouvez spécifier de 1 à 5, et la valeur par défaut est 3. Lorsque le nombre maximal de tentatives ayant échoué est dépassé, le système marque le serveur comme ayant échoué.

  Pour une fonctionnalité donnée, si vous avez configuré une méthode de secours à l'aide de la base de données locale et qu'aucun serveur du groupe ne répond, le groupe est considéré comme ne répondant pas et la méthode de secours est essayée. Le groupe de serveurs reste marqué comme ne répondant pas pendant la durée du temps mort, de sorte que les demandes AAA supplémentaires effectuées dans cette période ne résultent pas en une tentative d'entrer en contact avec le groupe de serveurs et que la méthode de secours est utilisée immédiatement.
- **Dynamic Authorization (Autorisation dynamique)** (pour VPN RA uniquement), **Port** : si vous activez les services d'autorisation dynamique ou de changement d'autorisation (CoA) RADIUS pour ce groupe de serveurs RADIUS, le groupe sera enregistré pour les notifications CoA et écoutera sur le port indiqué les mises à jour de la politique CoA provenant du Cisco Identity Services Engine (ISE). Le port d'écoute par défaut est 1700, ou vous pouvez définir un port différent dans l'intervalle 1024 à 65535. Activez

l'autorisation dynamique uniquement si vous utilisez ce groupe de serveurs dans un VPN d'accès à distance en conjonction avec l'ISE.

- **Realm that Supports the RADIUS Server** (Domaine qui prend en charge le serveur RADIUS) : si le serveur RADIUS est configuré pour utiliser un serveur AD afin d'authentifier les utilisateurs, sélectionnez le domaine AD qui spécifie le serveur AD utilisé avec ce serveur RADIUS. Si le domaine n'existe pas déjà, cliquez sur **Create New Identity Realm** (Créer un nouveau domaine d'identité au bas de la liste et configurez-le maintenant.
- **RADIUS Server list** (Liste des serveurs RADIUS : sélectionnez jusqu'à 16 objets serveur RADIUS qui définissent les serveurs du groupe. Ajoutez ces objets dans l'ordre de priorité. Le premier serveur de la liste est utilisé jusqu'à ce qu'il cesse de répondre. Après avoir ajouté les objets, vous pouvez faire glisser et déposer pour les réorganiser. Si l'objet n'existe pas encore, cliquez sur **Create New RADIUS Server** (Créer un nouveau serveur RADIUS) pour le créer maintenant.

  Vous pouvez également cliquer sur le lien **Test (Tester)** pour vérifier que le système peut se connecter au serveur. Vous êtes alors invité(e) à saisir un nom d'utilisateur et un mot de passe. Le test vérifie si le serveur peut être contacté et, si oui, que le nom d'utilisateur peut être authentifié.

Étape 4 (Facultatif) Cliquez sur le bouton **Test All Servers** (Tester tous les serveurs) pour vérifier la connectivité à chaque serveur du groupe.

Vous êtes alors invité(e) à saisir un nom d'utilisateur et un mot de passe. Le système vérifie si chaque serveur peut être contacté et si le nom d'utilisateur peut être authentifié sur chaque serveur.

Étape 5 Cliquez sur **OK**.

Dépannage des serveurs et groupes RADIUS

Voici quelques éléments que vous pouvez vérifier si l'autorisation extérieure ne fonctionne pas.

- Utilisez les boutons **Test** dans le serveur RADIUS et les objets de groupe de serveurs pour vérifier que les serveurs peuvent être contactés à partir du périphérique. Assurez-vous de sauvegarder les objets avant le test. Si le test échoue :
  - Veuillez comprendre que le test ne tient pas compte de l'interface configurée pour le serveur et utilise toujours l'interface de gestion. Le test devrait échouer si le serveur mandataire d'authentification RADIUS n'est pas configuré pour répondre aux demandes de l'adresse IP de gestion.
  - Vérifiez que vous saisissez une bonne combinaison nom d'utilisateur/mot de passe pendant le test. Vous devriez recevoir un message Bad Credentials (Mauvaises informations d'authentification) s'ils sont incorrects.
  - Vérifiez la clé secrète, le port et l'adresse IP du serveur. Si vous utilisez un nom d'hôte, vérifiez que le DNS est configuré pour l'interface de gestion. Envisagez la possibilité que la clé secrète ait été modifiée sur le serveur RADIUS, mais pas dans la configuration du périphérique.
  - Si le test continue d'échouer, vous devrez peut-être configurer une voie de routage statique vers les serveurs RADIUS. Essayez d'envoyer un message Ping au serveur à partir de la console d'interface de ligne de commande ou d'une session SSH pour voir s'il est possible de le joindre.

- Si l'authentification externe fonctionnait mais a cessé de fonctionner, envisagez la possibilité que tous les serveurs soient dans la période de délai mort. Lorsque tous les serveurs RADIUS d'un groupe ont échoué, « dead time » (délai mort) correspond au nombre de minutes pendant lesquelles le système attend avant de réessayer le premier serveur. Pendant le temps mort, l'authentification locale est utilisée, de sorte que le nom d'utilisateur et le mot de passe d'un utilisateur donné seraient le nom d'utilisateur et le mot de passe locaux. La valeur par défaut est de 10 minutes, mais vous pouvez configurer jusqu'à 1 440 minutes.
- Si l'authentification externe HTTPS fonctionne pour certains utilisateurs mais pas pour d'autres, évaluez l'attribut cisco-av-pair défini dans le serveur RADIUS pour chaque compte d'utilisateur. Cet attribut est peut-être mal configuré. Un attribut manquant ou incorrect bloquera tout accès HTTPS pour ce compte d'utilisateur.
- Si l'authentification externe SSH fonctionne pour certains utilisateurs mais pas pour d'autres, évaluez l'attribut Service-Type défini dans le serveur RADIUS pour chaque compte d'utilisateur. Cet attribut est peut-être mal configuré. Un attribut manquant ou incorrect bloquera tout accès SSH pour ce compte d'utilisateur.

Identity Services Engine (ISE)

Vous pouvez intégrer votre déploiement de Cisco Identity Services Engine (ISE) ou de ISE Passive Identity Connector (ISE-PIC) au Cisco Firewall Threat Defense pour utiliser ISE/ISE-PIC pour l'authentification passive.

ISE/ISE-PIC est une source d'identité faisant autorité et fournit des données de connaissance des utilisateurs pour les utilisateurs qui s'authentifient à l'aide d'Active Directory (AD), LDAP, RADIUS ou RSA. Cependant, pour Cisco Firewall Threat Defense, vous pouvez utiliser ISE pour connaître l'identité des utilisateurs en conjonction avec AD uniquement. Vous pouvez utiliser l'identité de l'utilisateur dans les politiques de contrôle d'accès et de déchiffrement SSL comme critères de correspondance, en plus de voir les informations de l'utilisateur dans les différents tableaux de bord et événements de surveillance.

Pour en savoir plus sur Cisco ISE/ISE-PIC, consultez le *Guide de l'administrateur de services d'identité Cisco Identity Services Engine* (https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html) et le *Guide d'installation et d'administration d'Identity Services Engine Passive Identity Connector (ISE-PIC)* (https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html).

Lignes directrices et limites pour ISE

- Le système de pare-feu ne prend pas en charge l'authentification 802.1x des périphériques en parallèle de l'authentification Active Directory, parce qu'il n'associe pas l'authentification des périphériques aux utilisateurs. Si vous utilisez des connexions actives 802.1x, configurez ISE pour signaler uniquement les connexions actives 802.1x (périphérique et utilisateur). De cette façon, une connexion de périphérique n'est signalée qu'une seule fois au système.
- ISE/ISE-PIC ne signale pas l'activité des utilisateurs des services invités ISE.
- Synchronisez l'heure sur le serveur ISE/ISE-PIC et sur le périphérique. Sinon, le système pourrait provoquer des expirations de délai d'utilisateur à des intervalles inattendus.
- Si vous configurez l'ISE/ISE-PIC pour surveiller un grand nombre de groupes d'utilisateurs, le système pourrait abandonner les mappages d'utilisateurs en fonction des groupes en raison des limites de mémoire.

Par conséquent, les règles assorties de conditions de domaine ou d'utilisateur peuvent ne pas fonctionner comme prévu.

- Pour connaître les versions précises d'ISE/ISE-PIC compatibles avec cette version du système, consultez le *Guide de compatibilité Cisco Secure Firewall*https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html,
- Utilisez l'adresse IPv4 du serveur ISE, sauf si vous confirmez que votre version d'ISE prend en charge IPv6.

Configurer Identity Services Engine (ISE)

Pour utiliser le moteur de services d'identité de Cisco (ISE) ou le connecteur d'identité passive du moteur de services d'identité de Cisco (ISE PIC) comme source d'identité passive, vous devez configurer la connexion au serveur ISE Platform Exchange Grid (pxGrid).

Avant de commencer

- Exportez les certificats de serveur pxGrid et MNT à partir d'ISE. Par exemple, dans ISE PIC 2.2, vous les trouvez sur la page **Certificates (Certificates)** > **Certificate Management (Gestion des certificats)** > **System Certificates (Certificats système)**. Le MNT (nœud de surveillance et de dépannage) est affiché comme Admin dans la colonne Utilisé par dans la liste des certificats. Vous pouvez soit les charger en tant que certificats d'autorité de certification de confiance sur la page **Objects (Objets)** > **Certificates (Certificats)**, soit les charger au cours de la procédure suivante. Ces nœuds peuvent utiliser le même certificat.
- Vous devez également configurer un domaine d'identité AD. Le système obtient la liste des utilisateurs d'AD et d'ISE il obtient des informations sur les mappages utilisateur-adresse IP.
- Si vous utilisez des balises de groupe de sécurité (SGT) pour le contrôle d'accès, avec ou sans mappages statiques de balises de groupe de sécurité, et si vous écoutez le sujet SXP, vous devez également configurer SXP et ces mappages dans ISE. Consultez Configurer les groupes de sécurité et la publication SXP dans ISE.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur **+** > **Identity Services Engine (Identity Services Engine)**. Vous pouvez créer au maximum un objet ISE.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Name** (Nom) : le nom de l'objet.

- **Status** (État) : cliquez sur la bascule pour activer ou désactiver l'objet. Lorsque cette option est désactivée, vous ne pouvez pas utiliser ISE comme source d'identité dans vos règles d'identité.
- **Description** : ajoutez une description facultative.
- **Primary Node Hostname/IP Address** (Nom d'hôte/adresse IP du nœud principal) : nom d'hôte ou adresse IP du serveur ISE pxGrid principal. Ne spécifiez pas d'adresse IPv6, sauf si vous avez vérifié que votre version d'ISE prend en charge IPv6.
- **Secondary Node Hostname/IP Address** (Nom d'hôte/adresse IP du nœud secondaire) : si vous configurez un serveur ISE secondaire pour la haute disponibilité, cliquez sur **Add Secondary Node Hostname/IP Address** (Ajouter un nom d'hôte/adresse IP de nœud secondaire) et saisissez le nom d'hôte ou l'adresse IP du serveur ISE pxGrid secondaire.
- **pxGrid Server CA Certificat**e (Certificat CA du serveur pxGrid) : le certificat de l'autorité de certification de confiance pour le cadre pxGrid. Si votre déploiement comprend un nœud pxGrid principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.
- **MNT Server CA Certificat**e (Certificat CA du serveur MNT : le certificat de l'autorité de certification de confiance pour le certificat ISE lors des téléchargements en bloc. Il peut s'agir du même certificat que celui du serveur pxGrid si votre serveur MNT (surveillance et dépannage) n'est pas distinct. Si votre déploiement comprend un nœud MNT principal et un nœud secondaire, les certificats des deux nœuds doivent être signés par la même autorité de certification.
- **Server Certificate** (Certificat du serveur) : le certificat d'identité interne que le périphérique Cisco Firewall Threat Defense doit fournir à ISE lors de la connexion à ISE ou lors des téléchargements en bloc.
- **Subscribe To (S'abonner à) :** sélectionnez les rubriques ISE pxGrid auxquelles vous devez vous abonner. S'abonner à une rubrique signifie que vous téléchargerez les données liées à cette rubrique.
  - **Session Directory Topic** (Rubrique Session Directory) : indique s'il faut obtenir des informations sur les sessions utilisateur, y compris les mappages SGT pour ces sessions. Par défaut, cette option est activée. Vous devez sélectionner cette option si vous souhaitez obtenir une identité d'utilisateur passive à utiliser dans les politiques de sécurité et pour la visibilité dans les tableaux de bord de surveillance.
  - **SXP Topic** (Rubrique SXP) : indique s'il faut obtenir des mappages statiques SGT–adresses IP. Sélectionnez cette rubrique si vous souhaitez écrire des règles de contrôle d'accès en fonction des balises de groupe de sécurité (SGT).
- **ISE Network Filters** (Filtres de réseau ISE) : filtre facultatif que vous pouvez définir pour restreindre les données qu'ISE transmet au système. Si vous fournissez un filtre de réseau, ISE ne signale que les données provenant des réseaux inclus dans ce filtre. Cliquez sur **+**, sélectionnez les objets réseau qui identifient les réseaux, puis cliquez sur **OK**. Cliquez sur **Create New Network** (Créer un nouveau réseau) si vous devez créer les objets. Configurez uniquement les objets réseau IPv4.

Étape 4 Cliquez sur le bouton **Test** pour vérifier que le système peut se connecter à votre serveur ISE.

Si le test échoue, cliquez sur le lien **See Logs** (Voir les journaux) pour lire les messages d'erreur détaillés. Par exemple, le message suivant indique que le système n'a pas pu se connecter au serveur sur le port requis. Le problème peut provenir de l'absence de route vers l'hôte, du fait que le serveur ISE n'utilise pas le port attendu ou de règles de contrôle d'accès qui empêchent la connexion.

```
Captured Jabberwerx log:2018-05-11T16:10:30 [   ERROR]: connection timed out while
```

```
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

Étape 5 Cliquez sur **OK** pour enregistrer l'objet.

Prochaine étape

Après avoir configuré ISE, activez la politique d'identité, configurez les règles d'authentification passive et déployez la configuration. Ensuite, vous devez accéder à ISE/ISE PIC et accepter le périphérique en tant qu'abonné. Si vous configurez ISE/ISE PIC pour accepter automatiquement les utilisateurs, vous n'avez pas besoin d'accepter manuellement l'abonnement.

Dépannage de la source d'identité ISE/ISE-PIC

Connexions ISE/ISE-PIC

Si vous rencontrez des problèmes avec la connexion ISE ou ISE-PIC, vérifiez les éléments suivants :

- La fonctionnalité de mappage d'identité pxGrid dans ISE doit être activée avant de pouvoir intégrer avec succès ISE au périphérique Cisco Firewall Threat Defense.
- Avant d'établir une connexion entre le serveur ISE et le périphérique Cisco Firewall Threat Defense, vous devez approuver manuellement les clients dans ISE.

  Vous pouvez également activer **Automatically approve new accounts** (Approuver automatiquement les nouveaux comptes) dans ISE, comme indiqué dans le chapitre sur la gestion des utilisateurs et des sources d'identité externes dans le *Guide de l'administrateur de Cisco Identity Services Engine*.
- Le certificat du périphérique Cisco Firewall Threat Defense (serveur) doit inclure la valeur d'utilisation de clé étendue **clientAuth** ou ne doit inclure aucune valeur d'utilisation de clé étendue. Si l'utilisation de clé étendue clientAuth est définie, aucune utilisation de clé ne doit être définie, ou la valeur d'utilisation de la clé de signature numérique (Digital Signature) doit être définie. Les certificats d'identité autosignés que vous pouvez créer à l'aide du Firepower Device Manager répondent à ces exigences.
- L'heure de votre serveur ISE doit être synchronisée avec l'heure sur le périphérique Cisco Firewall Threat Defense. Si les périphériques ne sont pas synchronisés, le système peut provoquer des délais d'expiration d'utilisateur à des intervalles imprévus.

Utilisateurs ISE/ISE-PIC

Si vous rencontrez des problèmes avec les données des utilisateurs signalées par ISE ou ISE-PIC, tenez compte des éléments suivants :

- Une fois que le système a détecté une activité d'un utilisateur ISE dont les données ne sont pas encore dans la base de données, le système récupère les informations à propos du serveur. L'activité vue par l'utilisateur ISE n'est pas gérée par les règles de contrôle d'accès et n'est pas affichée dans l'interface Web tant que le système n'a pas récupéré les informations la concernant lors d'un téléchargement d'utilisateur.
- Vous ne pouvez pas effectuer le contrôle utilisateur sur les utilisateurs ISE qui ont été authentifiés par un contrôleur de domaine LDAP, RADIUS ou RSA.
- Le système ne reçoit pas les données d'utilisateur pour les utilisateurs des services invités de Cisco ISE.

Serveurs SAML

Vous pouvez configurer les serveurs Security Assertion Markup Language 2.0 (SAML 2.0) pour les utiliser comme sources d'authentification par connexion unique (SSO) pour les connexions VPN d'accès à distance. SAML est une norme ouverte pour l'échange de données d'authentification et d'autorisation entre des parties, en particulier un fournisseur d'identité (IdP) et un fournisseur de services (SP).

Configurer les serveurs SAML

Vous pouvez configurer les serveurs Security Assertion Markup Language 2.0 (SAML 2.0) pour les utiliser comme sources d'authentification par connexion unique (SSO) pour les connexions VPN d'accès à distance. Par exemple, Duo Access Gateway (DAG) est un serveur SAML.

Lorsque vous utilisez un serveur SAML comme méthode d'authentification, le serveur SAML agit en tant que fournisseur d'identité (IdP), tandis que le périphérique Firewall Threat Defense agit en tant que fournisseur de services (SP).

Pour le VPN d'accès à distance, vous pouvez utiliser un serveur SAML comme source d'authentification principale, mais vous ne pouvez pas configurer une source d'authentification secondaire ni configurer une source de repli.

Avant de commencer

Obtenez les informations suivantes auprès du fournisseur d'identité du serveur SAML.

- URL de l'identifiant d'entité, qui fournit les métadonnées du serveur SAML.
- URL de connexion.
- URL de déconnexion.
- Certificat du fournisseur d'identité.

Le système ne prend pas en charge plusieurs valeurs renvoyées pour un attribut SAML. Par exemple, si vous utilisez SAML avec le VPN d'accès à distance, vous ne pouvez pas fournir plusieurs valeurs pour l'attribut de la stratégie de groupe Cisco : vous ne devez fournir qu'une seule valeur. Si vous envoyez plusieurs valeurs, une valeur par défaut est appliquée plutôt que de choisir l'une des valeurs fournies. Assurez-vous que le serveur SAML est configuré pour fournir une valeur unique pour chaque attribut renvoyé.

Procédure

Étape 1 Effectuez l'une des opérations suivantes pour accéder à la page des serveurs SAML :

- Sélectionnez **Objects** (Objets), puis **Identity Sources** (Sources d'identité) dans la table des matières.
- Sélectionnez **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)** > **SAML Servers (Serveurs SAML)**.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur **+** > **SAML Server** (Serveur SAML) .

- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Configurez les propriétés suivantes :

- **Name** (Nom) : le nom de l'objet.
- **Description** : ajoutez une description facultative.
- **URL de l'identifiant d'entité du fournisseur d'identité (IDP)** : l'URL d'une page qui sert le XML de métadonnées qui décrit comment l'émetteur SAML répondra aux demandes. Certains produits de serveur SAML l'appellent l'ID d'entité, d'autres l'appellent l'URL de métadonnées. L'URL doit comporter de 4 à 128 caractères, y compris le protocole, https://. Par exemple, https://191.168.2.21/dag/saml2/idp/metadata.php.
- **Sign-In URL** (URL de connexion) : l'URL pour la connexion au serveur du fournisseur d'identité SAML. L'URL doit comporter de 4 à 500 caractères, y compris le protocole. http:// et https:// sont autorisés. Par exemple, https://191.168.2.21/dag/saml2/idp/SSOService.php.
- **Sign-Out URL** (URL de déconnexion) : l'URL pour la déconnexion du serveur du fournisseur d'identité SAML. L'URL doit comporter de 4 à 500 caractères, y compris le protocole. http:// et https:// sont autorisés. Par exemple, https://191.168.2.21/dag/saml2/idp/SingleLogoutService.php.
- **Service Provider Certificate** (Certificat du fournisseur de services) : le certificat interne à utiliser pour le périphérique Firewall Threat Defense. Idéalement, vous avez déjà chargé un certificat signé par un tiers reconnu et vous pouvez le sélectionner maintenant. Vous pouvez également utiliser le certificat intégré DefaultInternalCertificate (Certificat interne par défaut), ou cliquer sur **Create New Internal Certificate** (Créer un nouveau certificat interne) et charger un certificat signé maintenant. Le fournisseur d'identité du serveur SAML devra faire confiance à ce certificat, vous devrez peut-être le charger sur le serveur SAML. Consultez la documentation du serveur SAML pour obtenir des renseignements sur la façon de charger des certificats ou d'activer une relation de confiance avec un fournisseur de services.
- **Identity Provider Certificate** (Certificat du fournisseur d'identité) : certificat de l'autorité de certification de confiance pour le fournisseur d'identité du serveur SAML. Téléchargez ce certificat à partir du serveur SAML. Si vous ne l'avez pas encore chargé, cliquez sur **Create New Trusted CA Certificate** (Créer un nouveau certificat d'AC de confiance) et chargez-le maintenant.
- **Request Signature** (Signature de la demande) : l'algorithme de chiffrement à utiliser lors de la signature de la demande de connexion. Sélectionnez Aucun pour désactiver le chiffrement. Sinon, choisissez l'un des éléments suivants, qui sont classés du plus faible au plus fort : SHA1, SHA256, SHA384, SHA512.
- **Request Timeout** (Délai d'expiration de la demande) : les assertions SAML ont une période de validité : l'utilisateur doit finaliser la demande d'authentification unique (SSO) dans ce délai. Vous pouvez définir un délai d'expiration, en secondes, pour changer cette période. Si vous définissez un délai d'expiration plus long que la condition NotOnOrAfter de l'assertion, votre délai d'expiration est ignoré, et la condition NotOnOrAfter est respectée. La plage est de 1 à 7 200 secondes. La valeur par défaut est de 300 secondes.
- **This SAML identity provider (IDP) is on an internal network** (Ce fournisseur d'identité SAML est sur un réseau interne) : indique si le serveur SAML fonctionne sur un réseau interne plutôt qu'à l'extérieur des réseaux protégés.
- **Request IDP re-authentication at login** (Demander une réauthentification IdP à la connexion) : sélectionnez cette option pour obliger l'utilisateur à se réauthentifier à chaque connexion, au lieu de

laisser le serveur SAML réutiliser une session d'authentification précédente. Par défaut, cette option est activée.

Étape 4 Cliquez sur **OK**.

Prochaine étape

Si vous avez activé **la fonction Demande de signature** pour chiffrer les communications, vous devez charger les informations du gestionnaire d'appareil sur le serveur SAML. Dans la liste des sources d'identité, cliquez sur le bouton **de téléchargement** ( ) pour le serveur et enregistrez le fichier XML. Ensuite, connectez-vous au serveur SAML et chargez les informations. Consultez la documentation de votre fournisseur SAML pour obtenir des informations détaillées.

Si vous utilisez le serveur pour la connexion au gestionnaire d'appareils et qu'il ne fonctionne pas, vérifiez la configuration du serveur SAML.

- Connectez-vous au fournisseur d'identité de SAML et vérifiez que le consommateur de réponse SAML du gestionnaire d'appareil est configuré correctement. La valeur doit être : https://<FDM_URL>/api/fdm/latest/fdm/token
- Si la signature est activée dans l'objet serveur SAML, assurez-vous que le certificat public du gestionnaire d'appareils est chargé dans l'application SAML et que le chiffrement est activé. Le chargement du fichier XML de gestionnaire d'appareil devrait ajouter le certificat au serveur SAML. Vous pouvez également récupérer le certificat du gestionnaire d'appareil par le biais de l'API FDM : https://<FDM_URL>/saml/metadata

Utilisateurs locaux

La base de données des utilisateurs locaux (LocalIdentitySource) comprend les utilisateurs que vous avez définis dans le Firepower Device Manager.

Vous pouvez utiliser des utilisateurs définis localement aux fins suivantes :

- Remote Access VPN (VPN d'accès à distance), en tant que source d'identité principale ou de secours.
- Management Access (Accès de gestion), en tant que source principale ou secondaire pour les utilisateurs Firepower Device Manager.

  L'utilisateur **admin** est un utilisateur défini localement par le système. Cependant, l'utilisateur admin ne peut pas se connecter à un VPN d'accès à distance. Vous ne pouvez pas créer d'utilisateurs administratifs locaux supplémentaires.

  Si vous définissez l'authentification extérieure pour l'accès de gestion, les utilisateurs externes qui se connectent au périphérique s'affichent dans la liste des utilisateurs locaux.
- Identity Policy (Politique d'identité), indirectement, en tant que source d'identité passive pour collecter l'identité des utilisateurs à partir des connexions VPN d'accès à distance.

Le sujet suivant explique comment configurer les utilisateurs locaux.

Configurer les utilisateurs locaux

Vous pouvez créer des comptes utilisateur directement sur le périphérique pour une utilisation avec le VPN d'accès à distance. Vous pouvez utiliser les comptes d'utilisateurs locaux au lieu ou en plus d'une source d'authentification externe.

Si vous utilisez la base de données d'utilisateurs locaux comme méthode d'authentification de repli pour le VPN d'accès à distance, veillez à configurer les mêmes noms d'utilisateur et mots de passe dans la base de données locale que les noms dans la base de données externe. Sinon, le mécanisme de repli ne sera pas efficace.

Les utilisateurs définis ici ne peuvent pas se connecter à l'interface de ligne de commande du périphérique.

Procédure

Étape 1 Sélectionnez **Objects (Objets)** > **Users (Utilisateurs)**.

La liste affiche les noms d'utilisateurs et les types de services, qui peuvent être :

- MGMT : pour les utilisateurs administrateurs qui peuvent se connecter à Firepower Device Manager. L'utilisateur admin est toujours défini et vous ne pouvez pas le supprimer. Vous ne pouvez pas non plus configurer d'utilisateurs MGMT supplémentaires. Toutefois, si vous définissez l'authentification extérieure pour l'accès de gestion, les utilisateurs externes qui se connectent au périphérique s'affichent dans la liste des utilisateurs locaux en tant qu'utilisateurs MGMT.
- VPN d'accès à distance : pour les utilisateurs qui peuvent se connecter à un VPN d'accès à distance configuré sur le périphérique. Vous devez également sélectionner la base de données locale pour la source principale ou secondaire (de repli).

Étape 2 Effectuez l'une des opérations suivantes :

- Pour ajouter un utilisateur, cliquez sur **+**.
- Pour modifier un utilisateur, cliquez sur l'icône de modification ( ) correspondant à l'utilisateur.

Si vous n'avez plus besoin d'un compte d'utilisateur particulier, cliquez sur l'icône de suppression ( ) pour l'utilisateur.

Étape 3 Configurez les propriétés de l'utilisateur :

Le nom et le mot de passe peuvent contenir n'importe quel caractère alphanumérique ou spécial ASCII imprimé, à l'exception des espaces et des points d'interrogation. Les caractères imprimés sont les codes ASCII 33 à 126.

- **Nom** : nom d'utilisateur pour la connexion au VPN d'accès à distance. Le nom peut comporter de 4 à 64 caractères et ne peut pas contenir d'espaces. Par exemple : jeanuntel.
- **Mot de passe** et **Confirmer le mot de passe** : Saisissez le mot de passe de l'utilisateur. Le mot de passe doit comporter de 8 à 16 caractères. Il ne peut pas contenir de lettres consécutives identiques. Il doit également contenir au moins un des éléments suivants : un chiffre, une majuscule, une minuscule et un caractère spécial.

Remarque

Les utilisateurs ne peuvent pas modifier leur mot de passe. Avisez-les de leurs mots de passe et, lorsqu'ils doivent les modifier, vous devez modifier le compte d'utilisateur. De plus, ne mettez pas à jour le mot de passe des utilisateurs MGMT externes : les mots de passe sont contrôlés par le serveur AAA externe.

Étape 4 Cliquez sur **OK**.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.